Statement

of

David Z. Bodenheimer, Esq.
Partner
Crowell & Moring LLP
Washington, DC

Before the

House Committee on Homeland Security's
Subcommittee on Management, Integration, & Oversight and
Subcommittee on Emergency Preparedness, Science, & Technology

Concerning

Helping Business Protect the Homeland: Is the Department of Homeland Security Effectively Implementing the SAFETY Act?

September 13, 2006

Introduction

Mr. Chairmen and Members of the Committee. Thank you for holding these hearings today on the Department of Homeland Security's implementation of the Support Anti-terrorism by Fostering Effective Technologies Act of 2002 (SAFETY Act). On the fifth anniversary of September 11th, we all understand and appreciate the vital role of the SAFETY Act in unleashing our technology to combat terrorism and protect the Homeland.

I am David Bodenheimer, a partner in the law firm of Crowell & Moring LLP in Washington, DC where I specialize in Government Contracts and Homeland Security. As part of this practice, I have advised clients, published articles, and lectured extensively on Homeland Security and SAFETY Act matters. In addition, I serve as Co-Chair of the ABA Science and Technology Section's Special Committee on Homeland Security. However, I appear before your Committee today in my personal capacity and the views that I express are my own.

This year, Secretary Chertoff and his team at the Department of Homeland Security (DHS) have made real progress in implementing the SAFETY Act by issuing final regulations in June, revising the application procedures in August, and approving SAFETY Act technologies at a more rapid pace. DHS deserves praise for these advances that bring the SAFETY Act closer to realizing its potential to expedite the development and deployment of anti-terrorism technology. However, the terrorists are not resting and neither can we. More remains to be done to better align the DHS implementation of the SAFETY Act with the Congressional intent to accelerate the availability of anti-terrorism technology by providing statutory protection from liability lawsuits arising out of terrorist acts. As discussed below, implementation of the SAFETY Act would benefit from the following enhancements:

- Assuring the Confidentiality of SAFETY Act Data
- Encouraging the Development of Breakthrough Technologies
- Synchronizing Procurements and SAFETY Act Approvals
- Extending the Duration of SAFETY Act Protection
- Establishing an Appeals Process

The SAFETY Act's Purpose to Promote Anti-Terrorism Technology

The DHS implementation of the SAFETY Act must be measured against the statutory purpose established by Congress. The SAFETY Act has a purpose that is both simple and clear – save lives through anti-terrorism technology. To clear the path for such technology to move from the drawing board to the "Nation's front-line defense," Congress created protections against liability lawsuits:

> The Select Committee [on Homeland Security] believes that technological innovation is the Nation's front-line defense against

> the terrorist threat. Unfortunately, the Nation's products liability system threatens to keep important new technologies from the market where they could protect our citizens. In order to ensure that these important technologies are available, the Select Committee believes that it is important to adopt a narrow set of liability protections for manufacturers of these important technologies.[1]
>
> * * *
>
> Briefly, the SAFETY Act ensures that U.S. companies will be able to develop and provide vital anti-terrorism technologies to help prevent or respond to terrorist attacks – without the threat of crippling lawsuits.[2]

This purpose rests upon a fundamental, Congressionally recognized premise – anti-terrorism technology is essential to Homeland defense.[3] Quite simply, we cannot secure over 100,000 miles of land and sea borders – much less our cyber borders – merely with guns, guards, and gates.[4] Only with technology can we tackle the gargantuan tasks of defending our vast borders and infrastructure against terrorism, while maintaining the flow of commerce, as mandated by the Homeland Security Act of 2002. Pub. L. No. 107-296, § 402(8), 116 Stat. 2178. Consequently, the appropriate question is whether the DHS implementation of the SAFETY Act fully and effectively serves this objective of fostering more anti-terrorism technology, more quickly, and more efficiently for Homeland Security.

In its final rule, DHS recognizes the purpose underlying the SAFETY Act: "The purpose of this rule is to facilitate and promote the development and deployment of anti-terrorism technologies that will save lives." 71 FED. REG. 33147 (June 8, 2006). While both the DHS final rule and revised application kit represent considerable improvements over their predecessors, further revisions must be made to assure that neither the spectre of crippling liability lawsuits nor the hurdles of the DHS review process foreclose or delay our access to the most robust arsenal of anti-terrorism tools.

DHS Enhancements for Opening the Anti-Terrorism Technology Pipeline

The following enhancements would serve the SAFETY Act's purpose by encouraging more companies to accelerate the pace of bringing the widest array of technology to our battle against terrorism.

Assuring the Confidentiality of SAFETY Act Applications & Data

In its earliest proposed rules on the SAFETY Act, DHS acknowledged "that successful implementation of the Act requires that applicants' intellectual property interests and trade secrets remain protected in the application process and beyond." 68 FED. REG. 41423 (July 11, 2003). In the latest rules, DHS has taken commendable steps to maintain the confidentiality of SAFETY Act application data by: (1) treating "the entirety of the application" as "confidential

under appropriate law"; (2) recognizing the applicability of various trade secret laws to the application information; and (3) committing to "utilize all appropriate exemptions from the Freedom of Information Act." 71 FED. REG. 33151, § N and 33168, § 25.10 (2006). However, DHS needs to take additional steps to assure SAFETY Act applicants that their most valuable technologies and secrets will be secure. Two key steps are: (1) establish a sound information security program; and (2) provide transparency and controls for any sharing of SAFETY Act data.

Information Security Program. A sound information security program is critical to avoid disincentives for companies to share SAFETY Act data about their most valuable technologies with DHS.[5] The new rules encourage electronic applications, but still do not address the concerns raised during the 2003 hearings on SAFETY Act implementation:

> We are also concerned that the Department has not clearly identified how it specifically will protect this sensitive proprietary data from unauthorized disclosure or dissemination . . . . While ITAA will certainly be the first to support and embrace the power of the Internet to enhance and transform business processes, the Internet is still an open system and is vulnerable to breaches. We are concerned that there is no mention of a comprehensive management plan to secure the systems over which data will be transmitted, policies and procedures applicable to DHS personnel operating and having access to the system, or details on the technological approaches the Department will take to secure the data provided by applicants. We urge the Department to work with industry to develop and implement a comprehensive plan to secure the data and network over which this highly sensitive, proprietary information will flow.[6]

These concerns have been magnified by cybersecurity issues that continue to challenge DHS, including: (1) failing scores on information security for the past two years on the Federal Information Security Management Act (FISMA) report card;[7] (2) continuing delays in filling the Assistant Secretary for Cybersecurity position;[8] and (3) various information security concerns identified by the Office of Management and Budget (OMB), GAO and the DHS Inspector General.[9] While the SAFETY Act regulations include DHS commitments to protect the confidentiality of applicant data, DHS needs to roll out a FISMA-compliant information security program built around the standards published by OMB and the National Institute of Standards and Technology (NIST).[10] With sound information security, DHS can better achieve the SAFETY Act purpose of encouraging more applicants to offer a broader array of technology due to their confidence that DHS will protect their confidential data.

Transparency & Controls for Information Sharing. In 2003, the interim SAFETY Act regulations stated that DHS "shall establish confidentiality protocols for maintenance and use of information submitted to the Department under the SAFETY Act and this part." 68 FED. REG. 59703, § 25.8 (2003). The final SAFETY Act regulations offer little more transparency or detail, stating that DHS "shall establish confidentiality procedures for safeguarding, maintenance and

use of information submitted to the Department under this part." 71 FED. REG. 33168, § 25.10(a) (2006).[11] These latest SAFETY Act regulations do not address industry concerns lingering from the 2003 SAFETY Act hearings regarding with whom DHS may share data, under what conditions, and with what controls in place. In both their testimony to Congress and comments to DHS, the major industry trade associations requested greater transparency and protection:

> The regulations should require DHS in every instance to provide advance notification to the submitter when considering whether to disclose SAFETY Act information to third parties, give the submitter the right to refuse to agree to disclosure of the information, and to seek judicial review of any decision to disclose the information before such disclosure is made.[12]

As the "focal point for the security of cyberspace" under Homeland Security Presidential Directive (HSPD) 7 (Dec. 7, 2003), DHS can demonstrate its leadership role in this area by establishing "best practices" for guarding the confidential information of SAFETY Act applicants. In particular, DHS should adopt SAFETY Act regulations that not only incorporate the industry requests above (notice, consent, and review), but should also include technical and management controls (*e.g.*, digital audits and watermarks) capable of tracking who received the data, which recipients signed non-disclosure agreements, what copies have been made, and when audits and training have been conducted. By publishing and implementing such rules governing SAFETY Act data, DHS will greatly enhance both its capability and credibility to protect this confidential information.

Encouraging Development of Breakthrough Technologies

The new regulations properly recognize the eligibility of developmental technology (*i.e.*, technology "that is being developed, tested, evaluated, modified or is otherwise being prepared for deployment") for SAFETY Act protection. 71 FED. REG. 33161, § 25.4(f) and 33156, § R (2006). However, these regulations and new Application Kit appear to establish an undue preference for existing technologies. At least six times, the Application Kit repeats the following statement emphasizing past or current sales as a critical factor in the approval process: "It may be very important and could significantly expedite your application if your Technology has been acquired or utilized (or is subject to an ongoing procurement) by the military, a Federal agency, or a state, local or foreign government entity." Application Kit at 21, 23, 27, 34, 35, 40 (July 2006). More worrisome, the new regulations create a second-class status for developmental technologies, imposing "limitations on the use and deployment" of such items, making approval "terminable at-will" by DHS, and generally restricting the duration of the designation ("presumptively not longer than 36 months"). 71 FED. REG. 33156, § R (2006).

The new SAFETY Act regulations and Application Kit send the wrong message, and create the wrong incentives, for companies building the anti-terrorism arsenal. Due to the heightened uncertainties in the SAFETY Act approval process for such breakthroughs, companies have greater incentive to invest their research dollars in anti-terrorism technology ready to be fielded now, rather than in breakthrough technologies that may revolutionize the war against terror. We cannot afford to focus the SAFETY Act approvals solely upon today's

technologies (*i.e.*, detecting conventional explosives) when the terrorists have moved on to nail polish and peroxide to build bombs in mid-air.[13] Furthermore, approvals burdened with "limitations" and "terminable at-will" conditions undermine the certainty needed to foster new anti-terrorism technologies, as the DHS rules acknowledge: "The Department is aware of this concern and understands that undependable or uncertain liability protections would not have the desired effect of fostering the deployment of anti-terrorism technologies." 71 FED. REG. 33152, § D (2006). As the purpose of the SAFETY Act is to provide "critical incentives for the **development** and deployment of anti-terrorism technologies" (71 FED. REG. 33147 (2006) (emphasis added)), development of such technologies should not be shortchanged.

In any event, the effort to distinguish between developmental and existing technologies may be illusory, as most technologies have elements of both:

> For example, many solutions evolve and cannot be completely defined or fixed in advance. It is therefore important to provide coverage when systems design, for instance, is part of the contract performance.[14]

Indeed, nearly all of the major Homeland Security programs include ongoing, evolutionary design and development work in parallel with other program activities.[15] As the president of one trade association explained, companies need to know during the design phase whether SAFETY Act protection is available:

> It is important that the regulations provide for QATT protection when systems design is part of the required contract performance. In the absence of such protection, Sellers may be unwilling to proceed.[16]

Thus, the DHS regulations and Application Kit should make clear that the SAFETY Act approval process will welcome both developmental and existing anti-terrorism technology and that companies will not be penalized in the application process for presenting breakthrough technologies for review and approval.

Synchronizing Procurements and SAFETY Act Approvals

In its latest regulations, DHS "recognizes the need to align consideration of SAFETY Act applications and the government procurement process more closely." 71 FED. REG. 33156, § P (2006). In addition, DHS has identified several procedures that should assist in accomplishing this objective, including (1) the option for agencies to seek "a preliminary determination of SAFETY Act applicability," (2) the use of "Block Designation or Block Certification," and (3) the potential that DHS "may expedite SAFETY Act review for technologies subject to ongoing procurement processes." 71 FED. REG. 33156, § P (2006). These procedures represent positive steps towards the critical objective of synchronizing procurements and SAFETY Act approvals. However, more needs to be done, as discussed below.

For companies selling anti-terrorism technology, the parallel track of procurements and SAFETY approvals presents substantial risks and uncertainties:

- Disqualification: Company is disqualified because it conditioned its bid upon receiving timely SAFETY Act approval;

- Delay: Company receives award prior to SAFETY Act approval, thus "betting the company" during the interim; or

- Default: Company receives contract award – but not SAFETY Act approval – forcing company either to default or to perform at risk.

According to an NDIA survey, "25 percent of the respondents had 'no bid' over 50 procurements because the company would be unable to obtain SAFETY Act protection in time for the procurement."[17] While such "no bid" actions may be less common with the accelerated pace of SAFETY Act approvals, the risk of losing opportunities for major technological advancements and breakthroughs must be carefully weighed in light of the purpose of the SAFETY Act.

In particular, DHS can foster the development and deployment of anti-terrorism technology by accepting the risk of delayed SAFETY Act approval. For example, DHS could offer indemnification under Public Law No. 85-804 or authorize bids contingent upon SAFETY Act approval.[18] By shouldering approval risks that fall almost entirely within its control, DHS would expand the field of competition and the array of anti-terrorism technologies available to both DHS and the public.

In addition, the approval process should benefit from a new position for a SAFETY Act technology advocate tasked with breaking bottlenecks, resolving impasses, and expediting critical applications. Such a technology advocate would reduce the risk of approval delays that plagued a similar process in the 1960's and 1970's when a small part of the Food & Drug Administration (FDA) review staff occasionally delayed life-saving drugs with excessive information demands.[19] In addition, a SAFETY Act technology advocate would help DHS to avoid the type of pitfalls encountered by the pharmaceutical industry when the FDA review staff found it easier to deny, than approve, applications.[20] With this technology advocate, the DHS objective would be directly aligned with Congressional intent that the SAFETY Act "Support" and "Foster" anti-terrorism technologies to save lives.

Extending the Duration of SAFETY Act Protection

Without identifying any support in the statute itself, the DHS final rule imposes a mandatory sunset period upon approved anti-terrorism technology, thus requiring renewal every "five to eight years" to maintain protection. 6 C.F.R. § 25.6(f), (h); 71 FED. REG. 33163-4 (2006). Since the time that DHS initially proposed this "five to eight year" period in 2003, industry consistently opposed it.[21]

DHS seeks to justify this rule based upon the assumption that the approval depends upon factors such as "a specific threat environment, the nature and cost of available insurance, and

other factors all of which are subject to change." 71 FED. REG. 33155, § N (2006). However, the factual basis for this assumption is unclear, as some technologies – like blast-proof glass and bomb-sniffing dogs – will change at glacial paces, if at all. If either the technology or the insurance requirements change, the DHS rules already impose reporting requirements that assure continued DHS supervision. 6 C.F.R. §§ 25.5(g), (h), 25.6(l), 71 FED. REG. 33162, 33165 (2006). If the threat environment changes, new technologies will replace the old. Thus, this agency-imposed restriction on the statute appears neither justified nor necessary.

In any event, the DHS mandatory sunset period cannot be squared with the express terms or purpose of the SAFETY Act. First, the SAFETY Act establishes statutory protections without any term limits. For example, the Act states that "No punitive damages . . . may be awarded," rather than that "No punitive damages . . . may be awarded **for five to eight years**." 6 U.S.C. § 442(b)(1). If Congress intended to limit the duration of statutory protections, the SAFETY Act surely would have said so. Second, the limited shelf-life for approved technologies will create a bow wave of renewals in five to eight years, burdening industry and DHS alike with paperwork and distracting both from the more important task of seeking and approving new technologies. Unless the review is a mere formality (in which case it is unnecessary), the additional burden and risk undermine the incentives for technology investments. Accordingly, the DHS renewal requirement runs counter to the statutory purpose of encouraging and facilitating the development and deployment of more technology more quickly.

Establishing an Appeals Process

Even for an arbitrary or unreasonable denial of a SAFETY Act application, the DHS rules cut off any opportunity for an administrative or judicial appeal. 6 C.F.R. § 25.9(c)(2), 71 FED. REG. 33167 (2006) ("Under Secretary's decision shall be final and not subject to review"). Instead, DHS suggests that an "interactive process" in which an applicant may "provide supplemental information and address issues" is "sufficient recourse." 71 FED. REG. 33155 § O (2006). Since 2003 when DHS proposed an "interactive process" without any appeal, the major trade associations expressed the need for an appeals process.[22]

This DHS policy of unreviewable denials is contrary to legislative intent favoring liberal approval, not rejection, of liability protection for anti-terrorism technology: "it is Congress' hope and intent that the Secretary will use the necessary latitude to make this list as broad and inclusive as possible, so as to insure that the maximum amount of protective technology and services become available."[23] Furthermore, this "no appeal" policy sends the wrong message, shielding the DHS reviewers from scrutiny or accountability for denying applications and discouraging companies from pursuing applications that may be denied without recourse. Finally, while DHS has accelerated the pace of approvals in the past year under Secretary Chertoff's leadership, the DHS rules do not include any procedural safeguards that would prevent a return to the period when DHS approved just six technologies in sixteen months.[24] Given the SAFETY Act's purpose to "save lives" through technology (71 FED. REG. 33147 (2006)), the right time for an appeals process is now, not after a terrorist incident causes us to regret the unavailability of a technology that could have protected us.

In the federal realm of agency actions, administrative or judicial review is the rule, not the exception. More than 50 years ago, agencies contended that rejection of a contractor's bid was too discretionary for external review, but the Court of Claims disagreed, instead recognizing a disappointed bidder's right to judicial review for breach of an agency's implied duty "to give fair and impartial consideration" to bid and proposal submissions. *Heyer Prods. Co. v. United States*, 135 Ct. Cl. 63, 69 (1956). In addition, agencies themselves have acknowledged the need for administrative or judicial review by establishing procedures for appeals and protests for everything from pesticides and pharmaceuticals to radio frequency (RF) devices and federal contract awards.[25] For SAFETY Act anti-terrorism technology designed to save lives, the case for a review or appeals process is at least equally compelling – if not more so.

Conclusion

Under Secretary Chertoff's leadership, DHS should be commended for bringing the SAFETY Act much closer to achieving its statutory purpose. With additional enhancements described above, the SAFETY Act can reach its full potential of facilitating the development and deployment of technologies essential to our fight against terrorism. I am available to answer your questions.

Endnotes

1 H.R. REP. NO. 107-609, Pt. 1, at 118 (July 24, 2002).

2 148 CONG. REC. E2079 (daily ed. Nov. 15, 2002) (statement of Rep. Armey).

3 *Border Technology: Keeping Terrorists Out of the United States: Hearing Before the Senate Subcomm. on Terrorism, Technology & Homeland Security and Subcomm. on Immigration, Border Security and Citizenship of the Comm. on the Judiciary*, 108th Cong., 1st Sess. 1-8 (Mar. 12, 2003) (statement of Sen. Kyl: "people can't possibly patrol the entire area, and therefore we are going to have to continue to enhance the application of technology") (statement of Sen. Feinstein: "technology is not the sole answer . . . but it is an essential element"); (statement of Sen. Kennedy: "We know that a great deal more has to be done in this area not only in getting the best technology, but also having it interoperable").

4 "The old security paradigm in this country of guns, gates, and guards is changing fast. And technology is going to replace it all." *Fiscal Year 2004 Homeland Security Appropriations: Hearings Before House Subcomm. on Homeland Security of Comm. on Appropriations*, 108th Cong., 1st Sess. (Mar. 20, 2003) (statement of Rep. Wamp).

5 With respect to critical infrastructure information, the Government Accountability Office (GAO) has documented instances in which industry does not share information with DHS due to concerns about "potential release of sensitive information" and uncertainty about how such information "will be used or protected from disclosure." GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 14 (July 19, 2005) (GAO-05-827T).

6 *Implementing the SAFETY Act: Advancing New Technologies for Homeland Security: Hearings before House Comm. on Government Reform*, 108th Cong., 1st Sess. 44 (statement of Mr. Miller) (hereinafter the "*2003 House SAFETY Act Hearings*").

[7] Rep. Davis, "No Computer System Left Behind: A Review of the 2005 Federal Computer Security Scorecards," House Comm. on Government Reform (Mar. 16, 2006) (http://reform.house.gov/UploadedFiles/TMD%20FISMA%2006%20Opener.pdf).

[8] Krebs, "A Year Later, Cybersecurity Post Still Vacant," *Washington Post*, p. A21 (July 13, 2006); "Democratic Senators, Industry Coalitions Urge DHS to Fill Still Vacant Cyber-Chief Slot," *BNA Privacy Law Watch* (July 14, 2006).

[9] OMB, *FY 2005 Report to Congress on Implementation of the Federal Information Security Management Act of 2002* at 39 (Mar. 1, 2006) (43% of DHS systems certified and accredited; 52% of security controls tested); *id* at 40 (DHS IG gave rating of "Poor" to DHS) (http://www.whitehouse.gov/omb/inforeg/reports/2005_fisma_report_to_congress.pdf); GAO, *Critical Infrastructure Protection: Challenges in Addressing Cybersecurity* 9-10 (July 19, 2005) (GAO-05-827T) (identification of DHS cybersecurity responsibilities and problem areas).

[10] OMB Circular No. A-130; OMB News Release, "OMB Reinforces Strict Adherence to Safeguard Standards" (June 26, 2006); OMB Memo to Department and Agency Heads, "Protection of Sensitive Agency Information" (June 23, 2006) (M-06-16) (www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf); NIST Special Publication 800-53A (2nd Public Draft) (Apr. 2006) (http://csrc.nist.gov/publications/drafts.html#sp800-53-Rev1).

[11] The DHS commitments to require non-disclosure agreements and to check for potential conflicts of interest are not new, as both the interim regulations in 2003 and the final regulations in 2006 address these issues. 68 FED. REG. 59687 (2003); 71 FED. REG. 33151 (2006).

[12] *2003 SAFETY Act Hearings* 54 (statement of Mr. Miller); *id.* at 150 (comments of Information Technology Association of America (ITAA), the Professional Services Council (PSC), the Aerospace Industries Association (AIA), and National Association of Manufacturers (NAM).

[13] "Technology isn't available to detect potentially lethal liquids hidden in sports drink bottles or other containers. The foiled airline attack from the U.K. highlighted the merits of good intelligence, which stopped the liquid bomb scheme before it reached a critical point." Alva, "Billions of Dollars Buy Tighter Security But Work Remains," *Investor's Business Daily* A1 (Sept. 11, 2006).

[14] *2003 House SAFETY Act Hearings* 58 (statement of Mr. Soloway).

[15] GAO, *Homeland Security: Progress Continues, but Challenges Remain on Department's Management of Information Technology* 30-31 (Mar. 29, 2006) (GAO-06-598T) (discussing challenges relating to requirements definition and development for major Homeland Security programs).

[16] *2003 House SAFETY Act Hearings* 65 (statement of Mr. Soloway).

[17] NDIA and PSC letter to DHS Under Secretaries Hale and McQueary dated Feb. 3, 2005.

[18] For the Secure Border Initiative (SBI) Net program, the DHS Request for Proposals specifically recognizes that the procurement should be covered by the SAFETY Act, but warns offerors that "Proposals in which pricing or any other term or condition is contingent upon

SAFETY Act protections of the proposed product(s) or service(s) will not be considered for award." In a number of other procurements, contractors have been disqualified for conditioning their proposals upon SAFETY Act approval.

[19] For example, in 1969, one FDA reviewing officer repeatedly demanded more data on the efficacy of aspirin in preventing heart attacks (including submission of all prior literature on aspirin), ultimately forcing E. R. Squibb & Sons, Inc. to abandon the research initiative. Wardell, "Rx: More Regulation or Better Therapies?" *Regulation* at 25-6 (Sept.-Oct. 1979). Five years later, studies by the National Institute of Health (NIH) confirmed substantial reductions in heart attacks attributable to aspirin, thus demonstrating the costs of unnecessary delays in the drug approval process. *Id.; see also* Elwood & Sweetnam, "Aspirin and Secondary Mortality After Myocardial Infarction," *The Lancet* 1313 (1979).

[20] The former FDA Commissioner described the incentives for FDA staff to take "negative action on new drug applications" as "intense" during the late 1960's. Grabowski, *Drug Regulation and Innovation* 76 (quoting speech by former FDA Commissioner Schmidt before the National Press Club in Washington, DC on Oct. 29, 1974).

[21] DHS does not explain why "five to eight years" represents an appropriate period of time. During hearings in 2003, the president of the ITAA objected to the "arbitrary timeframe for designation," adding alternatively that "we also believe that the timeframe should be extended to a minimum of 10 years – if not substantially longer – which is more consistent with the effective dates of long-term services agreements and more realistically reflects the length of time necessary to develop and implement complex systems and services." *2003 House SAFETY Act Hearings* 48 (statement of Mr. Miller). Similarly, the PSC president testified that "there is no public policy reason to impose any fixed period of time on the useful life of the Designation period of a QATT [qualified anti-terrorism technology]. Indeed, in some cases, a contract performance period can extend beyond five or eight years." *Id.* at 65 (statement of Mr. Soloway).

[22] *2003 House SAFETY Act Hearings* 55 (statement of Mr. Miller). In comments on the DHS proposed regulations in 2003, the ITAA, PSC, AIA, and NAM all requested an appeals process. *Id.* at 149.

[23] 148 CONG. REC. E2080 (daily ed. Nov. 15, 2002) (statement of Rep. Armey).

[24] "Shortly after being sworn in, Secretary of Homeland Security Michael Chertoff stated: 'There is more opportunity, much more opportunity, to take advantage of this important law, and we are going to do that.'" 71 FED. REG. 33148 (2006). During the earlier phase of SAFETY Act implementation "from October 2003 to February 2005, six technologies were designated Qualified Anti-Terrorism Technologies under the SAFETY Act." *Id.*

[25] 40 C.F.R. § 152.118(e) (2006) (right to hearing for denial of application for insecticide, fungicide or rodenticide); 47 C.F.R. §§ 1.106, 1.115 (2006) (petition for reconsideration by Federal Communications Commission (FCC) staff or for review by the FCC Commissioners for denial of RF equipment authorization); 21 C.F.R. §§ 201, 235 (2006) (hearing or judicial review for denial of a new drug application); Federal Acquisition Regulation (FAR) § 33.103 (agency review and alternative dispute procedures for disappointed bidders for federal contracts).